CLAIMS

What is claimed is:

1. An apparatus comprising:

a modular multiplier including a plurality of independent computation channels, said plurality of independent computation channels including a first computation channel and a second computation channel;

a coupling device interposed between said first computation channel and said second computation channel to receive a first control signal and to couple said first computation channel to said second computation channel in response to a receipt of said first control signal.

2. The apparatus as set forth in claim 1, wherein said modular multiplier comprises a linear systolic array of processing elements, said linear systolic array of processing elements including said plurality of independent computation channels.

3. The apparatus as set forth in claim 1, wherein said coupling device comprises a coupling device to receive a second control signal and to selectively couple said first computation channel to said second computation channel in response to a state of said second control signal.

4. The apparatus as set forth in claim 3, said apparatus having a first mode of operation corresponding to a first state of said second control signal wherein said first computation channel is operably separated from said second computation channel and a second mode of operation corresponding to a second state of said second control signal wherein said first computation channel is operably coupled to said second computation channel via said coupling device.

5. The apparatus as set forth in claim 4, wherein said first computation channel and said second computation channel operate as two n-bit modular multipliers in said first mode of operation and as a single 2n-bit modular multiplier in said second mode of operation, where n is an integer.

6. The apparatus as set forth in claim 5, where n is 512.

7. The apparatus as set forth in claim 1, wherein said modular multiplier comprises a Montgomery multiplier.

8. The apparatus as set forth in claim 1, wherein said a coupling device comprises a first multiplexer coupled between an output of said first computation channel and an input of said second computation channel and a second multiplexer coupled between an output of said second computation channel and an input of said first computation channel.

9. A processor comprising:

a modular multiplier including a plurality of independent computation channels, said plurality of independent computation channels including a first computation channel and a second computation channel;

a coupling device interposed between said first computation channel and said second computation channel to receive a first control signal and to couple said first computation channel to said second computation channel in response to a receipt of said first control signal.

10. The processor as set forth in claim 9, wherein said modular multiplier comprises a linear systolic array of processing elements, said linear systolic array of processing elements including said plurality of independent computation channels.

11. The processor as set forth in claim 9, wherein said coupling device comprises a coupling device to receive a second control signal and to selectively couple said first computation channel to said second computation channel in response to a state of said second control signal.

12. The processor as set forth in claim 11, said processor having a first mode of operation corresponding to a first state of said second control signal wherein said first computation channel is operably separated from said second computation channel and a

second mode of operation corresponding to a second state of said second control signal wherein said first computation channel is operably coupled to said second computation channel via said coupling device.

13. The processor as set forth in claim 12, wherein said first computation channel and said second computation channel operate as two n-bit modular multipliers in said first mode of operation and as a single 2n-bit modular multiplier in said second mode of operation, where n is an integer.

14. The processor as set forth in claim 13, where n is 512.

15. The processor as set forth in claim 9, wherein said modular multiplier comprises a Montgomery multiplier.

16. The processor as set forth in claim 9, wherein said a coupling device comprises a first multiplexer coupled between an output of said first computation channel and an input of said second computation channel and a second multiplexer coupled between an output of said second computation channel and an input of said first computation channel.

17. A system comprising:

a memory to store data and instructions;

a first processor coupled to said memory to process data and execute instructions; and

a second processor coupled to said memory, said second processor comprising:

a modular multiplier including a plurality of independent computation channels, said plurality of independent computation channels including a first computation channel and a second computation channel;

a coupling device interposed between said first computation channel and said second computation channel to receive a first control signal and to couple said first computation channel to said second computation channel in response to a receipt of said first control signal.

18. The system as set forth in claim 17, wherein said modular multiplier comprises a linear systolic array of processing elements, said linear systolic array of processing elements including said plurality of independent computation channels.

19. The system as set forth in claim 17, wherein said coupling device comprises a coupling device to receive a second control signal and to selectively couple said first computation channel to said second computation channel in response to a state of said second control signal.

20. The system as set forth in claim 19, said second processor having a first mode of operation corresponding to a first state of said second control signal wherein said first computation channel is operably separated from said second computation channel and a second mode of operation corresponding to a second state of said second control signal wherein said first computation channel is operably coupled to said second computation channel via said coupling device.

21. The system as set forth in claim 20, wherein said first computation channel and said second computation channel operate as two n-bit modular multipliers in said first mode of operation and as a single 2n-bit modular multiplier in said second mode of operation, where n is an integer.

22. The system as set forth in claim 17, wherein said a coupling device comprises a first multiplexer coupled between an output of said first computation channel and an input of said second computation channel and a second multiplexer coupled between an output of said second computation channel and an input of said first computation channel.

23. A method comprising:

receiving a first control signal and a plurality of operands; and

performing a modular multiplication operation on said plurality of operands utilizing a modular multiplier including a plurality of independent computation channels, said plurality of independent computation channels including a first computation channel

and a second computation channel, wherein performing said modular multiplication operation comprises:

coupling said first computation channel with said second computation channel in response to receiving said first control signal;

performing a first portion of said modular multiplication operation utilizing said first computation channel; and

performing a second portion of said modular multiplication operation utilizing said second computation channel.

24. The method as set forth in claim 23, wherein performing a modular multiplication operation comprises performing a modular multiplication operation on said plurality of operands utilizing a modular multiplier including a linear systolic array of processing elements, said linear systolic array of processing elements including said plurality of independent computation channels.

25. The method as set forth in claim 23, wherein:

performing a first portion of said modular multiplication operation comprises providing said plurality of operands to said first computation channel and processing said plurality of operands utilizing said first computation channel to produce an intermediate result;

coupling said first computation channel with said second computation channel comprises providing said intermediate result to said second computation channel; and

performing a second portion of said modular multiplication operation comprises processing said intermediate result utilizing said second computation channel.

26. The method as set forth in claim 23, said method further comprising receiving a second control signal, wherein coupling said first computation channel with said second computation channel comprises selectively coupling said first computation channel with said second computation channel in response to receiving said second control signal.

27. A machine-readable medium having a plurality of machine-executable instructions embodied therein which when executed by a machine, cause said machine to perform a method comprising:

receiving a first control signal and a plurality of operands; and

performing a modular multiplication operation on said plurality of operands utilizing a modular multiplier including a plurality of independent computation channels, said plurality of independent computation channels including a first computation channel and a second computation channel, wherein performing said modular multiplication operation comprises:

coupling said first computation channel with said second computation channel in response to receiving said first control signal;

performing a first portion of said modular multiplication operation utilizing said first computation channel; and

performing a second portion of said modular multiplication operation utilizing said second computation channel.

28. The machine-readable medium as set forth in claim 27, wherein performing a modular multiplication operation comprises performing a modular multiplication operation on said plurality of operands utilizing a modular multiplier including a linear systolic array of processing elements, said linear systolic array of processing elements including said plurality of independent computation channels.

29. The machine-readable medium as set forth in claim 27, wherein:

performing a first portion of said modular multiplication operation comprises providing said plurality of operands to said first computation channel and processing said plurality of operands utilizing said first computation channel to produce an intermediate result;

coupling said first computation channel with said second computation channel comprises providing said intermediate result to said second computation channel; and

performing a second portion of said modular multiplication operation comprises processing said intermediate result utilizing said second computation channel.

30. The machine-readable medium as set forth in claim 27, said method further comprising receiving a second control signal, wherein coupling said first computation channel with said second computation channel comprises selectively coupling said first

computation channel with said second computation channel in response to receiving said second control signal.